

AUS9-2000-0808-US1

**METHOD AND SYSTEM FOR MANAGING A DISTRIBUTED TRUST PATH
LOCATOR FOR PUBLIC KEY CERTIFICATES RELATING TO THE TRUST
PATH OF AN X.509 ATTRIBUTE CERTIFICATE**

5

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to an improved data processing system and, in particular, to a method and apparatus for multicomputer data transferring. Still more particularly, the present invention provides a method and apparatus for computer-to-computer authentication.

10

2. Description of Related Art

The commercial use of the Internet has dramatically increased the use of technology. Web-based and Internet-based applications have now become so commonplace that when one learns of a new product or service, one assumes that the product or service will incorporate Internet functionality into the product or service. New applications that incorporate significant proprietary technology are only developed when an enterprise has a significantly compelling reason for doing so. Many corporations have employed proprietary data services for many years, but it is now commonplace to assume that individuals and small enterprises also have access to digital communication services. Many of these services are or will be Internet-based, and the amount of electronic communication on the Internet is growing exponentially.

15

20

25

30

AUS9-2000-0808-US1

One of the factors influencing the growth of the Internet is the adherence to open standards for much of the Internet infrastructure. Individuals, public institutions, and commercial enterprises alike are able to introduce new content, products, and services that are quickly integrated into the digital infrastructure because of their ability to exploit common knowledge of open standards.

Concerns about the integrity and privacy of electronic communication have also grown with adoption of Internet-based services. Various encryption and authentication technologies have been developed to protect electronic communication. For example, an open standard promulgated for protecting electronic communication is the X.509 standard for digital certificates.

An X.509 digital certificate is an International Telecommunications Union (ITU) standard that has been adopted by the Internet Engineering Task Force (IETF) body. It cryptographically binds the certificate holder, presumably the subject name within the certificate, with its public cryptographic key. This cryptographic binding is based on the involvement of a trusted entity in the Internet Public Key Infrastructure (PKIX) called the "Certifying Authority". As a result, a strong and trusted association between the certificate holder and its public key can become public information yet remain tamper-proof and reliable. An important aspect of this reliability is a digital signature that the Certifying Authority stamps on a certificate before it is released for use. Subsequently, whenever the certificate is

AUS9-2000-0808-US1

presented to a system for use of a service, its signature is verified before the subject holder is authenticated. After the authentication process is successfully completed, the certificate holder may be provided access to certain information, services, or controller resources, i.e. the certificate holder may be authorized to access certain systems.

A standard for an X.509 Attribute Certificate has been proposed by which attribute certificates would be similar in structure to public key certificates but in which the attribute certificate would not contain a public key. An attribute certificate would be used to certify or otherwise securely bind a set of authorization capabilities to its subject holder. Those capabilities are possibly authenticated and then cryptographically verified by a target service sought by the holder of the attribute certificate, and the attribute certificate may then be used for enabling access to controlled resources.

Within the prior art, establishing a trust path in an attribute certificate requires the presence of the public key certificates for the attribute certificate's issuing authority as well as that of the user of the attribute certificate. Administrative management and processing of information associated with these trust paths can be complex, and the deployment of a standard public key infrastructure is already hampered by the cost of the complexity of the public key infrastructure.

Therefore, it would be advantageous to have a method and system that simplifies the administrative processing associated with the trust paths that are required for valid use of attribute certificates. It would be

AUS9-2000-0808-US1

particularly advantageous to enable a user to carry and present an attribute certificate without simultaneously carrying and presenting the public key certificates that are required by the attribute certificate.

AUS9-2000-0808-US1

SUMMARY OF THE INVENTION

A method and a system is presented for managing attribute certificates. A target service within a distributed data processing system receives an attribute certificate from a client. A first locator is retrieved from the attribute certificate; the first locator identifies a location of a public key certificate of an issuing authority for the attribute certificate. The public key certificate of the issuing authority for the attribute certificate is then retrieved from the specified location. The attribute certificate is then verified by using the public key certificate of the issuing authority for the attribute certificate. The client is then authorized to have access to the controlled resources in the target service in accordance with authorization attributes stored in the attribute certificate.

An extension within an attribute certificate, called a distributed trust path locator, allows an attribute certificate to be physically disassociated from its supporting public key certificates while remaining logically associated with its supporting public key certificates. The user's attribute certificate and its supporting PKCs allows any server using an attribute certificate to locate and retrieve the PKC of the user and of the AC-issuing authority. The user is not required to communicate his/her PKC to a target service. In addition, configuring the target service to accept attribute certificates does not require the deployment of a PKC for every AC-issuing authority.

AUS9-2000-0808-US1

BRIEF DESCRIPTION OF THE DRAWINGS

The novel features believed characteristic of the invention are set forth in the appended claims. The invention itself, further objectives, and advantages thereof, will be best understood by reference to the following detailed description when read in conjunction with the accompanying drawings, wherein:

Figure 1A depicts a typical distributed data processing system in which the present invention may be implemented;

Figure 1B depicts a typical computer architecture that may be used within a data processing system in which the present invention may be implemented;

Figure 2 depicts a typical manner in which an entity obtains a digital certificate;

Figure 3A is a block diagram depicting a typical manner in which an entity may use a digital certificate to be authenticated to an Internet system or application;

Figure 3B is a block diagram depicting a typical manner in which an entity may use a digital certificate and an accompanying attribute certificate to be authenticated and authorized to an Internet system or application in order to be granted access to controller resources;

Figure 4 depicts a block diagram showing a method of using an attribute certificate with a Distributed Trust Path Locator in accordance with a preferred embodiment of the present invention;

AUS9-2000-0808-US1

Figure 5A shows some of the fields of a standard X.509 digital certificate;

Figures 5B-5C show some of the fields of an X.509 attribute certificate;

5 **Figure 6** shows the structure of a Distributed Trust Path Locator for use within an X.509 attribute certificate in accordance with a preferred embodiment of the present invention; and

10 **Figure 7** shows a flowchart depicting the processing of an attribute certificate for authorizing a certificate holder on a system using the Distributed Trust Path Locator methodology of the present invention.

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192

AUS9-2000-0808-US1

DETAILED DESCRIPTION OF THE INVENTION

With reference now to the figures, **Figure 1A** depicts
5 a typical network of data processing systems, each of
which may implement the present invention. Distributed
data processing system 100 contains network 101, which is
a medium that may be used to provide communications links
between various devices and computers connected together
10 within distributed data processing system 100. Network
101 may include permanent connections, such as wire or
fiber optic cables, or temporary connections made through
telephone or wireless communications. In the depicted
example, server 102 and server 103 are connected to
15 network 101 along with storage unit 104. In addition,
clients 105-107 also are connected to network 101.
Clients 105-107 and servers 102-103 may be represented by
a variety of computing devices, such as mainframes,
personal computers, personal digital assistants (PDAs),
20 etc. Distributed data processing system 100 may include
additional servers, clients, routers, other devices, and
peer-to-peer architectures that are not shown.

In the depicted example, distributed data processing
system 100 may include the Internet with network 101
25 representing a worldwide collection of networks and
gateways that use various protocols to communicate with
one another, such as Lightweight Directory Access Protocol
(LDAP), Transport Control Protocol/Internet Protocol
(TCP/IP), Hypertext Transport Protocol (HTTP), Wireless
30 Application Protocol (WAP), etc. Of course, distributed
data processing system 100 may also include a number of

AUS9-2000-0808-US1

different types of networks, such as, for example, an intranet, a local area network (LAN), or a wide area network (WAN). For example, server 102 directly supports client 109 and network 110, which incorporates wireless communication links. Network-enabled phone 111 connects to network 110 through wireless link 112, and PDA 113 connects to network 110 through wireless link 114. Phone 111 and PDA 113 can also directly transfer data between themselves across wireless link 115 using an appropriate technology, such as Bluetooth™ wireless technology, to create so-called personal area networks (PAN) or personal ad-hoc networks. In a similar manner, PDA 113 can transfer data to PDA 107 via wireless communication link 116.

The present invention could be implemented on a variety of hardware platforms; **Figure 1A** is intended as an example of a heterogeneous computing environment and not as an architectural limitation for the present invention.

With reference now to **Figure 1B**, a diagram depicts a typical computer architecture of a data processing system, such as those shown in **Figure 1A**, in which the present invention may be implemented. Data processing system 120 contains one or more central processing units (CPUs) 122 connected to internal system bus 123, which interconnects random access memory (RAM) 124, read-only memory 126, and input/output adapter 128, which supports various I/O devices, such as printer 130, disk units 132, or other devices not shown, such as a audio output system, etc. System bus 123 also connects communication adapter 134 that provides access to communication link 136. User

AUS9-2000-0808-US1

interface adapter 148 connects various user devices, such as keyboard 140 and mouse 142, or other devices not shown, such as a touch screen, stylus, microphone, etc. Display adapter 144 connects system bus 123 to display device 146.

Those of ordinary skill in the art will appreciate that the hardware in **Figure 1B** may vary depending on the system implementation. For example, the system may have one or more processors, such as an Intel® Pentium®-based processor and a digital signal processor (DSP), and one or more types of volatile and non-volatile memory. Other peripheral devices may be used in addition to or in place of the hardware depicted in **Figure 1B**. In other words, one of ordinary skill in the art would not expect to find similar components or architectures within a Web-enabled or network-enabled phone and a fully featured desktop workstation. The depicted examples are not meant to imply architectural limitations with respect to the present invention.

In addition to being able to be implemented on a variety of hardware platforms, the present invention may be implemented in a variety of software environments. A typical operating system may be used to control program execution within each data processing system. For example, one device may run a Unix® operating system, while another device contains a simple Java® runtime environment. A representative computer platform may include a browser, which is a well known software application for accessing hypertext documents in a variety of formats, such as graphic files, word processing files, Extensible Markup

AUS9-2000-0808-US1

Language (XML), Hypertext Markup Language (HTML), Handheld Device Markup Language (HDML), Wireless Markup Language (WML), and various other formats and types of files.

Hence, it should be noted that the distributed data processing system shown in **Figure 1A** is contemplated as being fully able to support a variety of peer-to-peer subnets and peer-to-peer services.

The present invention may be implemented on a variety of hardware and software platforms, as described above. More specifically, though, the present invention is directed to providing an authorization methodology that secures user access to applications or systems within a distributed data processing environment. To accomplish this goal, the present invention uses the trusted relationships associated with digital certificates in a novel manner to authorize user access for an application or system. Before describing the present invention in more detail, though, some background information about digital certificates is provided for evaluating the operational efficiencies and other advantages of the present invention.

Digital certificates support public key cryptography in which each party involved in a communication or transaction has a pair of keys, called the public key and the private key. Each party's public key is published while the private key is kept secret. Public keys are numbers associated with a particular entity and are intended to be known to everyone who needs to have trusted interactions with that entity. Private keys are numbers that are supposed to be known only to a particular entity, i.e. kept secret. In a typical public

AUS9-2000-0808-US1

key cryptographic system, a private key corresponds to exactly one public key.

Within a public key cryptography system, since all communications involve only public keys and no private
5 key is ever transmitted or shared, confidential messages can be generated using only public information and can be decrypted using only a private key that is in the sole possession of the intended recipient. Furthermore,
public key cryptography can be used for authentication,
10 i.e. digital signatures, as well as for privacy, i.e. encryption.

Encryption is the transformation of data into a form unreadable by anyone without a secret decryption key; encryption ensures privacy by keeping the content of the
15 information hidden from anyone for whom it is not intended, even those who can see the encrypted data. Authentication is a process whereby the receiver of a digital message can be confident of the identity of the sender and/or the integrity of the message.

20 For example, when a sender encrypts a message, the public key of the receiver is used to transform the data within the original message into the contents of the encrypted message. A sender uses a public key to encrypt data, and the receiver uses a private key to decrypt the
25 encrypted message.

When authenticating data, data can be signed by computing a digital signature from the data and the private key of the signer. Once the data is digitally signed, it can be stored with the identity of the signer
30 and the signature that proves that the data originated from the signer. A signer uses a private key to sign

AUS9-2000-0808-US1

data, and a receiver uses the public key to verify the signature. The present invention is directed to a form of authentication using digital certificates; some encryption is also performed during the processing within
5 the present invention.

A certificate is a digital document that vouches for the identity and key ownership of entities, such as an individual, a computer system, a specific server running on that system, etc. Certificates are issued by
10 certificate authorities. A certificate authority (CA) is an entity, usually a trusted third party to a transaction, that is trusted to sign or issue certificates for other people or entities. The CA usually has some kind of legal responsibilities for its
15 vouching of the binding between a public key and its owner that allow one to trust the entity that signed a certificate. There are many such certificate authorities, such as VeriSign, Entrust, etc. These authorities are responsible for verifying the identity
20 and key ownership of an entity when issuing the certificate.

If a certificate authority issues a certificate for an entity, the entity must provide a public key and some information about the entity. A software tool, such as
25 specially equipped Web browsers, may digitally sign this information and send it to the certificate authority. The certificate authority might be a company like VeriSign that provides trusted third-party certificate authority services. The certificate authority will then
30 generate the certificate and return it. The certificate may contain other information, such as dates during which

AUS9-2000-0808-US1

the certificate is valid and a serial number. One part of the value provided by a certificate authority is to serve as a neutral and trusted introduction service, based in part on their verification requirements, which are openly published in their Certification Service Practices (CSP).

Typically, after the CA has received a request for a new digital certificate, which contains the requesting entity's public key, the CA signs the requesting entity's public key with the CA's private key and places the signed public key within the digital certificate. Anyone who receives the digital certificate during a transaction or communication can then use the public key of the CA to verify the signed public key within the certificate. The intention is that an entity's certificate verifies that the entity owns a particular public key.

The X.509 standard is one of many standards that defines the information within a certificate and describes the data format of that information. The "version" field indicates the X.509 version of the certificate format with provision for future versions of the standard. This identifies which version of the X.509 standard applies to this certificate, which affects what information can be specified in it. Thus far, three versions are defined. Version 1 of the X.509 standard for public key certificates was ratified in 1988. The version 2 standard, ratified in 1993, contained only minor enhancements to the version 1 standard. Version 3, defined in 1996, allows for flexible extensions to certificates in which certificates can be extended in a

AUS9-2000-0808-US1

standardized and generic fashion to include additional information.

In addition to the traditional fields in public key certificates, i.e. those defined in versions 1 and 2 of X.509, version 3 comprises extensions referred to as "standard extensions". The term "standard extensions" refers to the fact that the version 3 of the X.509 standard defines some broadly applicable extensions to the version 2 certificate. However, certificates are not constrained to only the standard extensions, and anyone can register an extension with the appropriate authorities. The extension mechanism itself is completely generic.

Other aspects of certificate processing are also standardized. The Certificate Request Message Format (RFC 2511) specifies a format recommended for use whenever a relying party is requesting a certificate from a CA. Certificate Management Protocols have also been promulgated for transferring certificates. More information about the X.509 public key infrastructure (PKIX) can be obtained from the Internet Engineering Task Force (IETF) at www.ietf.org.

With reference now to **Figure 2**, a block diagram depicts a typical manner in which an individual obtains a digital certificate. User 202, operating on some type of client computer, has previously obtained or generated a public/private key pair, e.g., user public key 204 and user private key 206. User 202 generates a request for certificate 208 containing user public key 204 and sends the request to certifying authority 210, which is in possession of CA public key 212 and CA private key 214.

AUS9-2000-0808-US1

Certifying authority 210 verifies the identity of user 202 in some manner and generates X.509 digital certificate 216 containing signed user public key 218 that was signed with CA private key 214. User 202 receives newly generated digital certificate 216, and user 202 may then publish digital certificate 216 as necessary to engage in trusted transactions or trusted communications. An entity that receives digital certificate 216 may verify the signature of the CA by using CA public key 212, which is published and available to the verifying entity.

With reference now to **Figure 3A**, a block diagram depicts a typical manner in which an entity may use a digital certificate to be authenticated to an Internet system or application. User 302 possesses X.509 digital certificate 304, which is transmitted to an Internet or intranet application 306 that comprises X.509 functionality for processing and using digital certificates and that operates on host system 308. The entity that receives certificate 304 may be an application, a system, a subsystem, etc. Certificate 304 contains a subject name or subject identifier that identifies user 302 to application 306, which may perform some type of service for user 302.

Host system 308 may also contain system registry 310 which is used to authorize user 302 for accessing services and resources within system 308, i.e. to reconcile a user's identity with user privileges. For example, a system administrator may have configured a user's identity to belong to certain a security group,

AUS9-2000-0808-US1

and the user is restricted to being able to access only those resources that are configured to be available to the security group as a whole. Various well-known methods for imposing an authorization scheme may be employed within the system.

In order to facilitate the separation of authentication functions and authorization functions, a standard for an X.509 Attribute Certificate (AC) has been proposed by which attribute certificates (ACs) would be similar in structure to public key certificates (PKCs) but in which the attribute certificate would not contain a public key. An attribute certificate would be used to certify or otherwise securely bind a set of authorization capabilities to its subject holder. Those capabilities are possibly authenticated and then cryptographically verified by a target service sought by the holder of the attribute certificate, and the attribute certificate may then be used for enabling access to controlled resources.

A common analogy using passports and visas has been widely disseminated to explain the differences between public key certificates and attribute certificates. A public key certificate can be analogized to a passport: each identify the holder of the document; each have relatively long validity periods; and each require significant effort to obtain a valid document.

In contrast, an attribute certificate can be analogized to a visa. A visa is used to gain access somewhere in a manner similar to using an attribute certificate to gain access to a system. In addition, a visa must be accompanied by a passport that verifies/authenticates the identity of the holder of the

AUS9-2000-0808-US1

passport and the visa. Similarly, an attribute certificate must be accompanied by a public key certificate to verify/authenticate the identity of the user. A visa is issued by an authority other than the authority that issues a passport, which is similar to an attribute certificate being issued by an authority different from the authority that issues the public key certificate. A visa and an attribute certificate have shorter validity periods than a passport or a public key certificate.

Public key certificates can provide an identity for controlled access purposes. However, merely proving one's identity does not provide one with access to a controlled resource. Instead, a role or group-membership is used; if the user can prove one's identity and that the identity has been previously associated with a role or a group membership, then one may gain access to a controlled resource.

Although it is possible to do so, placing authorization information in a public key extension can be problematic. For example, a user may have a valid identity for a relatively long period of time, but the user's authorized access privileges may change over time with each authorization period being shorter than the valid period of time for the user's identity. If one were to place the authorization information in a public key extension, then the public key certificate would have to be reissued, which would cause a significant administrative burden.

Another problem, as was noted above, is that the authority that issues the public key certificate to

AUS9-2000-0808-US1

verify the identity of a person is usually not the same authority that desires to authorize that person. In fact, a preferred scheme would have relatively few public key certifying authorities on which many other
5 institutions rely while determining the authorization parameters for each individual institution. If the authorization information is placed into a public key extension, then the public key certifying authority must obtain authorization information from each institution to
10 which the user desires to present the public key certificate, which is very difficult administratively.

Hence, it has been recognized that the public key infrastructure would be better served by separating authorization information from authentication
15 information. However, authorization information must still be bound to a holder's identity to be useful.

In order to facilitate such a scheme, an attribute certificate provides a binding between a certificate holder and a set of attributes; the attribute certificate
20 is a digitally signed (or certified) identity and set of attributes. After acquiring an attribute certificate, a user may present the attribute certificate in an attempt to gain access to a controlled resource. When a decision must be made concerning whether a user should have access
25 to the controlled resource, the deciding authority needs to verify the identity of the holder of the attribute certificate.

Hence, an attribute certificate is generally presented along with a public key certificate to access
30 various security services, access controlled services, authentication services, etc. The attribute certificate

AUS9-2000-0808-US1

contains some type of information that links the attribute certificate with a public key certificate, and the public key certificate is used for authentication purposes in conjunction with a request to access the controlled resource.

With reference now to **Figure 3B**, a block diagram depicts a typical manner in which an entity may use an attribute certificate and its associated public key certificates to be authenticated and authorized to an Internet system or application in order to be granted access to controller resources. User 352 possesses X.509 attribute certificate 354. User 352 sends attribute certificate 354, along with the user's associated PKC 356 and PKC 358 of the issuing authority for the user's attribute certificate, to Internet or intranet application 360 that comprises X.509 functionality and that operates on host system 362. As noted previously, an attribute certificate may contain attributes that specify group membership, role, security clearance, or other authorization information associated with the holder of the attribute certificate. Host system 362 may also contain system registry 364 that allows user 352 to access services and resources within system 360 as specified by information within attribute certificate 354.

In summary of the prior art methodology, an X.509 attribute certificate is a document that has been cryptographically signed by an AC-issuing authority. This signing process uses the private key of the attribute certificate authority, for which there is a

AUS9-2000-0808-US1

corresponding public key published in a public key certificate issued for the attribute-certificate-issuing authority.

In the prior art, an application service that
5 contains PKIX-functionality uses the public key certificate of the user in conjunction with some predefined security protocol in order to establish data origin authenticity/integrity or confidentiality during exchanges with a particular client. At some subsequent
10 point in time, a user may attempt to access a controlled resource at a target service, and the user's access capabilities are determined from the user's attribute certificate. In the prior art, the user sends both
15 his/her attribute certificate and public key certificate to the target service. The two certificates are linked together in some manner; in the X.509 specification, the "Holder" field in the attribute certificate contains linking information for the public key certificate, such as the identity of the public key certificate's issuing
20 authority and the serial number of the holder's public key certificate.

After receiving the user's certificates, the public key certificate of the authority that issued the attribute certificate is needed in order to validate the
25 attribute certificate that has been presented by the user. In general, the target service would be configured with information on all of the AC-issuing authorities that the target service is willing to accept or trust.

In contrast with the prior art methods of using an
30 attribute certificate, such as that shown in **Figure 3B**, the present invention provides a novel method by which a

AUS9-2000-0808-US1

user simply carries an attribute certificate while a targeted application server seamlessly determines the location from which to download the public key certificates involved with the validation of the attribute certificate. The present invention introduces the use of a "Distributed Trust Path Locator" for an attribute certificate to accomplish this novel functionality, as explained below in more detail.

The present invention allows the user to send only his/her attribute certificate to the target service; the attribute certificate may contain an indication of the location of the user's public key certificate associated with the user's attribute certificate as well as an indication of the location of the AC-issuing authority's public key certificate, i.e. the AC may contain a Distributed Trust Path Locator. These locations, or locators, are placed within the attribute certificate when the attribute certificate is first generated. The indicated locations are then used by the target service to automatically locate and download the user's PKC and the AC-issuing authority's PKC.

With reference now to **Figure 4**, a block diagram shows a method of using an attribute certificate with a Distributed Trust Path Locator in accordance with a preferred embodiment of the present invention. **Figure 4** merely provides a graphic manner of depicting the additional functionality provided by the present invention compared to prior art methodologies as shown in **Figure 3B**.

User 402 is a valid holder of attribute certificate 404, which user 402 presents to target service 406 to

AUS9-2000-0808-US1

access a controlled resource. Target service 406 extracts PKC_LOCATOR 408, which is a Distributed Trust Path Locator, and uses PKC_LOCATOR 408 to locate a database or directory service, such as directory 410, that stores the PKCs that are needed by target service 406 to validate attribute certificate 404. Directory 410 then returns user's PKC 412 and PKC 414 of the issuing authority of attribute certificate 404. It should be noted that the user's PKC and the AC-issuing authority's PKC are not necessarily stored within the same directory or database, i.e. PKC_LOCATOR 408 may contain separate locations for both PKCs.

With the present invention, a PKIX-enabled application server is not required to be configured with the AC-issuing authority public key certificates of the AC-issuing authorities that the application server trusts. Furthermore, there is no limit to what a server can trust with respect to AC-issuing authorities as long as the validation chains of the required public key certificates lead to trusted PKIX certifying authorities. Ultimately, the validation steps should lead to constructing the X.509 PKC chain leading to the root trusted certifying authority for both the PKC of the AC-issuing authority as well as the user's PKC.

With reference now to **Figure 5A**, some of the fields of a standard X.509 digital certificate are shown. The constructs shown in **Figure 5A** are in Abstract Syntax Notation 1 (ASN.1) and are defined within the X.509 standard.

AUS9-2000-0808-US1

With reference now to **Figures 5B-5C**, some of the fields of an X.509 attribute certificate are shown. The constructs shown in **Figures 5B-5C** are also in ASN.1 notation.

5 With reference now to **Figure 6**, a diagram shows the structure of a Distributed Trust Path Locator for use within an X.509 attribute certificate in accordance with a preferred embodiment of the present invention. The attribute certificate contains the Distributed Trust Path

10 Locator that is used at the target service to determine and acquire the public key certificates necessary in the attribute certificate validation process. In the preferred embodiment, the Distributed Trust Path Locator is inserted as an extension in the standard extensions

15 field of the associated attribute certificate, as shown in **Figure 6** using ASN.1 notation. The "PKClocator" field in **Figure 6** is similar to the PKC_LOCATOR data item shown in **Figure 4**. The "PKClocator" field contains two data items: a locator for the PKC of the holder of the

20 attribute certificate; and a locator for the PKC of the issuing authority of the attribute certificate. The content within the locator may have a variety of formats, as shown in **Figure 6**. An application server uses the attribute certificates' PKClocator extension to locate

25 the distributed PKC of the AC-issuing authority and possibly that of the user if so desired. The location is generic enough to allow for different types of network or local locations, most notably a directory name that can point to an LDAP (Lightweight Directory Access Protocol)

30 service URI.

AUS9-2000-0808-US1

It should be noted that the Distributed Trust Path Locator is not limited to being incorporated within only the X.509 standard and that the X.509 standard is merely one set of definitions of digital certificates in which the Distributed Trust Path Locator of the present invention could be incorporated; the present invention may also use other digital certificate standards or formats other than X.509 as long as the digital certificates can convey the required information.

Moreover, the Distributed Trust Path Locator does not necessarily have to be incorporated as an extension into an X.509 attribute certificate, and that over time, as the X.509 standard changes, the Distributed Trust Path Locator of the present invention could become a standard field of an attribute certificate. Additionally, it should be noted that the format of the extension containing the Distributed Trust Path Locator could vary from the format shown in **Figure 6**.

With reference now to **Figure 7**, a flowchart depicts the processing of an attribute certificate for authorizing a certificate holder on a system using the Distributed Trust Path Locator methodology of the present invention. The processing begins in **Figure 7** with a user at a client system sending an attribute certificate to a server supporting a target service (step 702). The target service extracts the Distributed Trust Path Locator from the attribute certificate (step 704), from which the locator for the user's PKC is extracted (step 706) and the locator for the AC-issuing authority's PKC is also extracted (step 708).

AUS9-2000-0808-US1

It should be noted again that a locator for the user's PKC does not necessarily have to be included in the attribute certificate if it is not required by the target service to authenticate the user. However, in order to verify the attribute certificate, the AC-issuing authority's PKC must be obtained.

The target service then retrieves the user's PKC from the location specified by the extracted locator for the user's PKC (step 710), and the target service also retrieves the AC-issuing authority's PKC from the location specified by the extracted locator for AC-issuing authority's PKC (step 712). The order in which the PKCs are retrieved is not relevant, and the PKCs may be retrieved in parallel. After receiving the PKCs, the target service verifies the attribute certificate using the retrieved PKCs (step 714), and assuming that the verification is successful, then the target service may allow the user or client to have access to the controlled resource's of the target service in accordance with the authorization attributes in the user's attribute certificate (step 716). The process of authorizing the client through an attribute certificate using a Distributed Trust Path Locator is then complete.

The advantages of the present invention should be apparent in view of the detailed description of the invention that is provided above. By using a novel extension within an attribute certificate called a distributed trust path locator, the present invention allows an attribute certificate to be physically disassociated from its supporting public key certificates while remaining logically associated with its supporting

AUS9-2000-0808-US1

public key certificates. The present invention couples the user's attribute certificate and its supporting PKCs in a way that allows any server using an attribute certificate to locate and retrieve the PKC of the user and of the AC-issuing authority. The user is not required to communicate his/her PKC to a target service. In addition, configuring the target service to accept attribute certificates does not require the deployment of a PKC for every AC-issuing authority.

The methodology provided by the present invention is particularly useful to smaller, portable devices, such as Internet-enabled phones and PDAs which have less storage space and simpler applications. The present invention does not contribute any additional complexity to the usage model and certificate validation process of PKIX than the prior art methodologies for using attribute certificates.

It is important to note that while the present invention has been described in the context of a fully functioning data processing system, those of ordinary skill in the art will appreciate that the processes of the present invention are capable of being distributed in the form of instructions in a computer readable medium and a variety of other forms, regardless of the particular type of signal bearing media actually used to carry out the distribution. Examples of computer readable media include media such as EPROM, ROM, tape, paper, floppy disc, hard disk drive, RAM, and CD-ROMs and transmission-type media, such as digital and analog communications links.

AUS9-2000-0808-US1

The description of the present invention has been presented for purposes of illustration but is not intended to be exhaustive or limited to the disclosed embodiments. Many modifications and variations will be apparent to those of ordinary skill in the art. The
5 embodiments were chosen to explain the principles of the invention and its practical applications and to enable others of ordinary skill in the art to understand the invention in order to implement various embodiments with
10 various modifications as might be suited to other contemplated uses.